



9110-9P P

**DEPARTMENT OF HOMELAND SECURITY**

**Docket No. CISA-2019-0013**

**CISA Reporting Forms**

**AGENCY:** Cybersecurity Division (CSD), Cybersecurity and Infrastructure Security Agency (CISA), Department of Homeland Security (DHS).

**ACTION:** 60-Day Notice and Request for Comments; Revision, 1670-0037

**SUMMARY:** DHS CISA CSD will submit the following Information Collection Request (ICR) to the Office of Management and Budget (OMB) for review and clearance in accordance with the Paperwork Reduction Act of 1995.

**DATES:** Comments are encouraged and will be accepted until *[INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]*.

**ADDRESSES:** You may submit comments, identified by docket number CISA-2019-0013, by one of the following methods:

- **Federal eRulemaking Portal:**

<http://www.regulations.gov>. Please follow the instructions for submitting comments.

- **E-mail:** [fed\\_ir\\_update@hq.dhs.gov](mailto:fed_ir_update@hq.dhs.gov). Please include docket number CISA-2019-0013 in the subject line of the message.

- **Mail:** Written comments and questions about this Information Collection Request should be forwarded to DHS/CISA/CSD, ATTN: 1670-0037, 245 Murray Lane, SW, Mail Stop 0613, Washington, DC 20598-0613.

*Instructions:* All submissions received must include the words "Department of Homeland Security" and the docket number for this action. Comments received will be posted without alteration at <http://www.regulations.gov>, including any personal information provided.

*Docket:* For access to the docket and comments received, please go to [www.regulations.gov](http://www.regulations.gov) and enter docket number CISA-2019-0013.

Comments submitted in response to this notice may be made available to the public through relevant websites. For this reason, please do not include in your comments information of a confidential nature, such as sensitive personal information or proprietary information. If you send an e-mail comment, your e-mail address will be automatically captured and included as part of the comment that is placed in the public docket and made available on the Internet. Please note that responses to this public comment request containing any routine notice about the confidentiality of the communication will be treated as public comments that may be made available to the public

notwithstanding the inclusion of the routine notice.

**FOR FURTHER INFORMATION CONTACT:** Lisa Barr at 703.705.6078  
or at [fed\\_ir\\_update@hq.dhs.gov](mailto:fed_ir_update@hq.dhs.gov).

**SUPPLEMENTARY INFORMATION:** Section 2209 of the Homeland Security Act, as amended, established a national cybersecurity and communications integration center to function as "a Federal civilian interface for the multi-directional and cross-sector sharing of information related to cyber threat indicators, defensive measures, cybersecurity risks, incidents, analysis, and warnings for Federal and non-Federal entities." 6 U.S.C. 659(c)(1). The Federal Information Security Modernization Act of 2014 (FISMA) establishes a federal information security incident center, and requires the Department to operate it. 44 U.S.C. 3556(a).

The Cybersecurity and Infrastructure Security Agency (CISA) operates the federal information security incident center. Through this center, FISMA requires the Department to provide technical assistance and guidance on detecting and handling security incidents, compile and analyze incident information that threatens information security, inform agencies of current and potential threats and vulnerabilities, and provide intelligence or other information about cyber threats, vulnerabilities, and

incidents to agencies. 44 U.S.C. 3556(a). FISMA also requires agencies to report information security incidents, major incidents, and data breaches to the federal information security incident center. 44 U.S.C. 3556(b) (information security incidents), 44 U.S.C. 3554(b) (7) (C) (iii) (III) (major incidents); Pub. L. No. 113-283, 2(d) (2014) (codified at 44 U.S.C. 3553, note (Breaches)). The Cybersecurity Information Sharing Act of 2015 (CISA 2015) requires DHS, in consultation with interagency partners, to establish the Federal Government's capability and process for receiving cyber threat indicators and defensive measures, and directs DHS to further share cyber threat indicators and defensive measures it receives with certain federal entities in an automated and real-time manner. 6 U.S.C. 1504(c).

CISA is responsible for performing, coordinating, and supporting response to information security incidents, which may originate outside the Federal community and affect users within it, or originate within the Federal community and affect users outside of it. Often, therefore, the effective handling of security incidents relies on information sharing among individual users, industry, and the Federal Government, which may be facilitated by and through CISA.

Per the Federal Information Security Modernization Act of 2014, CISA operates the Federal information security incident center for the United States federal government. Each federal agency is required to notify and consult with CISA regarding information security incidents involving the information and information systems (managed by a federal agency, contractor, or other source) that support the operations and assets of the agency. Additional entities report incident information to CISA voluntarily.

CISA's website (at [US-CERT.gov](https://us-cert.gov)) is a primary tool used by constituents to report incident information, access information sharing products and services, and interact with CISA. Constituents, which may include anyone or any entity in the public, use forms located on the website to complete these activities.

By accepting incident reports and feedback, and interacting among federal agencies, industry, the research community, state and local governments, and others to disseminate reasoned and actionable cyber security information to the public, CISA has provided a way for citizens, businesses, and other institutions to communicate and coordinate directly with the Federal Government about cybersecurity. The information is collected via the following forms:

1. The Incident Reporting Form, DHS Cyber Threat Indicator and Defensive Measure Submission System and Malware Analysis Submission Form enable end users to report incidents and indicators as well as submit malware artifacts associated with incidents to CISA. This information is used by DHS to conduct analyses and provide warnings of system threats and vulnerabilities, and to develop mitigation strategies as appropriate. The primary purpose for the collection of this information is to allow DHS to contact requestors regarding their request.
2. The Mail Lists Form enables end users to subscribe to the National Cyber Awareness System's mailing lists, which deliver the content of and links to CISA's information sharing products. The user must provide an e-mail address in order to subscribe or unsubscribe, though both of these actions are optional. The primary purpose for the collection of this information is to allow DHS to contact requestors regarding their request.
3. The Cyber Security Evaluation Tool (CSET) Download Form, which requests the name, e-mail

address, organization, infrastructure sector, country, and intended use of those seeking to download the CSET. All requested fields are optional. The primary purpose for the collection of this information is to allow DHS to contact requestors regarding their request.

In order to be responsive to an ever-changing cybersecurity environment, the forms may change to collect data related to current capabilities or vulnerabilities. Standards, guidelines, and requirements of the CISA are perpetually adapting to the volatile cybersecurity environment. We must retain the ability to update these forms as required, or we will be unable to collect critical incident data in support of our mission. Without the necessary tools and methods to collect this information, we will be unable to effectively satisfy mission requirements and support our stakeholders through information collection, analysis, and exchange. The general scope and purpose of the forms will remain the same.

Incident reports are primarily submitted using CISA's Automated Indicator Sharing program. Alternately, information may be collected through web-based electronic forms, email, or telephone. Web form submission is also used as the collection method for the other forms listed.

These methods enable individuals, private sector entities, personnel working at other federal or state agencies, and international entities, including individuals, companies and other nations' governments to submit information.

This is a revision to an existing form. The changes to the collection since the previous OMB approval include: updating the name of the Agency from NPPD to CISA, updating the Incident Reporting Form, removing the ICSJWG FORM, and updating the burden and cost estimates.

The Incident Reporting Form was updated to add reporting options; and updated to improve user-friendliness by having the form be directional. The changes include: adding structured, distinct options for reporting incidents, major incidents, breaches, and events under investigation; and adding fields to collect expanded information on topics including attack vectors, indicators of compromise, communications from compromised systems, critical infrastructure sectors, memory captures, system and network logs, and unattributed cyber intrusions.

This is a revised information collection.

OMB is particularly interested in comments that:

1. Evaluate whether the proposed collection of information is necessary for the proper performance of the functions of the agency,



including whether the information will have practical utility;

2. Evaluate the accuracy of the agency's estimate of the burden of the proposed collection of information, including the validity of the methodology and assumptions used;
3. Enhance the quality, utility, and clarity of the information to be collected; and
4. Minimize the burden of the collection of information on those who are to respond, including through the use of appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology, e.g., permitting electronic submissions of responses.

*Title of Collection:* CISA Reporting Forms

*OMB Control Number:* 1670-0037

*Frequency:* Annually

*Affected Public:* State, Local, Tribal, and Territorial Governments, Private Sector, and Academia

*Number of Annualized Respondents:* 139,125

*Estimated Time Per Respondent:* 0.3333 hours, 0.1667 hours,  
or 0.0167 hours

*Total Annualized Burden Hours: 13,852 hours*

*Total Annualized Respondent Opportunity Cost: \$504,494*

*Total Annualized Respondent Out-of-Pocket Cost: \$0*

*Total Annualized Government Cost: \$2,100,032*

**Scott Libby,**

*Deputy Chief Information Officer.*

[FR Doc. 2019-19022 Filed: 9/3/2019 8:45 am; Publication Date: 9/4/2019]